⚠ DEADLINE: JUNE 30, 2026

Colorado AI Act
Compliance Checklist

SB 24-205 requires deployers of high-risk AI systems to have impact assessments, consumer notices, and grievance processes in place. This checklist covers every deployer obligation.

REGULOME.IO · 2026 EDITION · FREE DISTRIBUTION

Who is covered by the *Colorado AI Act?*

> ⚠ **Enforcement begins June 30, 2026**
>
> The Colorado AI Act applies to any business deploying high-risk AI systems that make or substantially influence consequential decisions affecting Colorado residents — regardless of where the company is headquartered.

A "high-risk AI system" under Colorado law is one that makes, or is a substantial factor in making, a **consequential decision**. The law creates obligations for both **developers** (who build the AI) and **deployers** (who use it), with deployers bearing the primary compliance burden.

Deployers (primary obligations)

- → Any business using AI to make consequential decisions
- → Applies regardless of company headquarters location
- → Must conduct impact assessments
- → Must provide consumer notice and disclosure
- → Must establish grievance and appeal processes
- → Must implement risk management programs
- → Must publish public statement on AI use

Developers (supporting obligations)

- → AI system builders and vendors
- → Must provide deployers with documentation
- → Must disclose known limitations and risks
- → Must share training data information
- → Must notify deployers of known discrimination risks
- → Must cooperate with deployer impact assessments

Consequential decision areas

- → Employment and hiring decisions
- → Educational opportunities and admissions
- → Financial services and credit decisions
- → Healthcare access and treatment
- → Housing and rental decisions
- → Insurance underwriting and claims
- → Legal services access

Penalties and enforcement

- → Enforced by the Colorado Attorney General
- → Civil penalties for non-compliance
- → Violations treated as deceptive trade practices
- → Affirmative defense available if reasonable compliance efforts demonstrated
- → No private right of action (AG enforcement only)
- → Penalties assessed per violation

SB 24-205

COLORADO AI ACT · DEPLOYER OBLIGATIONS

Compliance Checklist

8 requirements every deployer of high-risk AI must complete before June 30, 2026. Use the Status and Notes columns to track your organization's progress.

☐	REQUIREMENT	STATUS	NOTES
☐	**Identify all high-risk AI systems in your stack** — Map every AI system that makes or substantially influences consequential decisions affecting Colorado residents. Include vendor-provided tools. Prioritize employment, credit, healthcare, and housing contexts.		
☐	**Complete an AI impact assessment for each high-risk system** — Conduct an impact assessment covering the system's intended purpose, known limitations, potential for algorithmic discrimination, and performance metrics. Document and retain.		
☐	**Implement a risk management program** — Establish documented policies and procedures to manage algorithmic discrimination risks — with designated ownership and review cadence.		
☐	**Provide consumer notice before consequential decisions** — Notify Colorado consumers that an AI system is being used to make or assist a consequential decision. Notice must be given prior to or contemporaneous with the decision.		
☐	**Disclose the type of AI system and its role in the decision** — Consumers have the right to know the nature of the AI system. Upon request, provide the principal reason(s) for the decision and the data that contributed to it.		
☐	**Establish a grievance and appeal process** — Consumers must have a meaningful opportunity to appeal consequential decisions made using high-risk AI. Create a formal process for receiving, reviewing, and responding to appeals.		
☐	**Conduct annual bias and discrimination reviews** — Perform an annual review of each high-risk AI system for algorithmic discrimination. Consider engaging third-party auditors for objectivity.		
☐	**Publish a public statement on high-risk AI use** — Post a clear public statement summarizing the types of high-risk AI systems deployed and how you manage associated risks. Typically published on your website privacy or AI governance page.		

DEV

COLORADO AI ACT · DEVELOPER OBLIGATIONS

Developer Checklist

If you build or sell AI systems used by deployers to make consequential decisions, these requirements apply to you.

☐	REQUIREMENT	STATUS	NOTES
☐	**Provide deployers with system documentation** — Supply documentation describing system capabilities, limitations, intended uses, known risks, and performance characteristics.		
☐	**Disclose training data information** — Provide deployers with information about the data used to train and validate the AI system, including data sources and known biases.		
☐	**Notify deployers of known discrimination risks** — Proactively inform deployers of any known or reasonably foreseeable risks of algorithmic discrimination.		
☐	**Cooperate with deployer impact assessments** — Make available the information deployers need to complete their AI impact assessments. Respond to deployer inquiries in a timely manner.		

GUIDE

COLORADO AI ACT · REQUIRED DOCUMENTATION

Impact Assessment Template

The Colorado AI Act requires deployers to complete and maintain an impact assessment for each high-risk AI system. Use this as a starting template for your documentation.

☐	IMPACT ASSESSMENT ELEMENT	STATUS	NOTES
☐	**System purpose and use case** — Document the intended purpose of the AI system, the consequential decision it supports, and the context of deployment.		
☐	**Affected population** — Identify and describe the Colorado consumers affected by the system's decisions, including demographic breakdown where available.		
☐	**Data inputs and features** — Document the data inputs used by the system, including proxy variables that may correlate with protected characteristics.		
☐	**Known limitations and failure modes** — Document known system limitations, edge cases, failure modes, and the potential for algorithmic discrimination.		
☐	**Performance metrics and evaluation** — Document the metrics used to evaluate system performance, including fairness metrics across demographic groups.		
☐	**Mitigation measures** — Document the measures in place to mitigate risks of algorithmic discrimination, including human oversight mechanisms.		
☐	**Consumer notice mechanism** — Document how affected consumers are notified that AI is involved in the decision and how they can request more information.		
☐	**Appeal process documentation** — Document the process for consumers to appeal decisions, including response timelines and escalation paths.		
☐	**Review schedule** — Document the planned review cadence for the impact assessment (annually at minimum) and the trigger events for off-cycle reviews.		
☐	**Responsible parties** — Name the individuals or roles responsible for maintaining the impact assessment, conducting reviews, and acting on findings.		

Affirmative defense tip

The Colorado AI Act provides an affirmative defense for deployers who can demonstrate they made reasonable efforts to comply. Maintaining thorough, dated impact assessments — even if imperfect — strengthens this defense. Start now, iterate later.

Find *AI compliance* advisors

Regulome lists AI compliance consultants, auditors, and legal advisors. Compare providers, check their specializations, and get quotes — all in one place.

regulome.io